Privacy Background

Contents

I. Purpose and Design of this Module

The Presidential Commission for the Study of Bioethical Issues (Bioethics Commission) conducts research and develops reports and other materials for public distribution in order to advise and counsel the President of the United States on bioethical issues that arise as a consequence of advances in biomedicine and related areas of science and technology. To support ethics education and facilitate the integration of bioethical analysis into existing curricula across traditional and nontraditional educational and professional settings, we have developed pedagogical materials designed to increase distribution of the Bioethics Commission's work and

to facilitate easy access to the material in its reports by professors, instructors, teachers, and professional leaders (collectively "instructors").

This module was prepared for instructors who want to include in their teaching a discussion of privacy. It provides foundational information, ethical reasoning, applications, questions, discussion points, and additional readings that are designed to give the instructor enough information to plan lectures, discussions, or activities. These materials are not intended to be a lecture script or outline, but rather to support the instructor in developing his or her own presentation(s).

In addition to the background information provided here, further modules provide a guide for instructors to facilitate incorporation of the Bioethics Commission's published reports as a resource for teaching and discussion. The featured Bioethics Commission reports illustrate relevant and current applications of privacy in various contexts.

Instructors are invited to use these materials, or any portion of them, to integrate bioethics into coursework and professional development activities in all disciplines. Feedback is welcome, including insight into how the materials have been used and suggestions for how they might be improved for use in the future. (Send feedback to education@bioethics.gov.)

II. Introduction

All individuals have certain types of information that they feel comfortable sharing and other types of information that they prefer to keep private. Although the line distinguishing what to keep private and what to share might be different for each of us, we all recognize the importance of being able to keep some information private. But what exactly does it mean to keep things private?

There is no consensus on the definition of privacy. Privacy seemingly embodies a number of ideals, including the right to control flows of information and the right to make decisions free from outside interference. Embedded within discussions of privacy are considerations of confidentiality, anonymity, and data protection. These varied notions raise ethical, philosophical, and legal questions about what precisely is or should be private and when individuals have a right to privacy.

The United States offers privacy protections for specific, circumscribed areas, whereas other countries have more comprehensive legal privacy protections. The U.S. Supreme Court has recognized constitutional rights of privacy based on interpretations of the Bill of Rights and the 14th Amendment. For example, the right to privacy comes into play with respect to making fundamental decisions without governmental interference—decisions involving choosing who to marry and with whom to procreate—and the right to be free from certain governmental searches.

The United States also offers some statutory protections for individuals that cover specific areas, including educational records, credit histories, and health information.

Health information presents particular privacy challenges, due in part to its sensitive nature. As health information is increasingly stored electronically, many of the same impulses that motivated stricter statutory privacy protections in other areas could potentially motivate increasing privacy protections for health information.

III. Learning Objectives

Students should be able to:

1. Describe the history of privacy protections in the United States.
2. Discuss the various practical, philosophical, ethical, and legal notions embedded in and related to the idea of privacy.
3. Describe the Bioethics Commission's guiding ethical principles and the ways in which they relate to privacy.
4. Describe key legal cases and laws that shape the right to privacy in the United States.
5. Discuss ways in which the U.S. approach to privacy differs from the European approach.
6. Discuss the specific privacy concerns raised by health information.

IV. Background

A. History of Privacy

Concerns about privacy date as far back as ancient Greece and Rome: Aristotle, for example, distinguished between public and private, as did ancient Roman law.[1] Modern philosophical thinking about privacy owes much to John Stuart Mill, who argued that society ought not intervene in one's private acts except to protect others from harm.[2]

[1] DeCew, J. (2013). Privacy. In E.N. Zalta. (Ed.). *The Stanford Encyclopedia of Philosophy* (Fall 2013 Edition). Retrieved October 6, 2014 from http://plato.stanford.edu/entries/privacy/; Allen, A.L. (1999). Coercing privacy. *William & Mary Law Review*, 40(3), 723-757. Retrieved October 6, 2014 from http://scholarship.law.wm.edu/wmlr/vol40/iss3/3/.

[2] Mill, J.S. (2003). *Of the Limits to Authority of Society over the Individual.* In D. Bromwich and G. Kateb. (Eds.). On Liberty (pp. 139-155). New Haven, CT: Yale University Press.

In the United States, the seminal article on privacy, "The Right to Privacy," was written by Samuel Warren and future Supreme Court Justice Louis Brandeis, and published in the *Harvard Law Review*.[3] The article responded to concerns about "modern enterprise and invention"—namely, cameras taking snapshots, and the subsequent publication of those photos—invading an individual's privacy.[4] Warren and Brandeis argued that U.S. law should recognize a privacy right, or a "right to be let alone."[5]

William Prosser's 1960 article "Privacy," published in the *California Law Review*, was another milestone. This influential article described four "intrusion of privacy" common law torts that emerged as the result of about three hundred state court decisions in the United States.[6]

The first tort, intrusion upon seclusion, protects individuals from wrongful encroachment into their private affairs.[7] The second tort, public disclosure of private facts, protects individuals from the publication of embarrassing or highly sensitive private facts about them that are not otherwise newsworthy.[8] These torts apply only to facts that are entitled to be private and for which a reasonable person would consider intrusion or disclosure highly offensive.[9] The third tort, publicity that portrays someone in a false light, protects individuals from false or misleading statements made with reckless disregard to the truth that a reasonable person would consider highly offensive.[10] The last of the four torts, appropriation of name or likeness, applies if a person or entity uses an individual's name, likeness or identity for their own benefit or advantage.[11]

These four torts—intrusion upon seclusion, public disclosure of private facts, publicity which portrays someone in a false light, and appropriation of name, likeness or identity—are incorporated into the *Restatement (Second) of Torts* issued by the American Law Institute.[12] Most states have adopted all or part of the invasion of privacy torts.[13] These four tort law causes

[3] Warren, S.D., and L.D. Brandeis. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193-220.
[4] Warren, S.D., and L.D. Brandeis, op cit, pp. 195-196.
[5] Warren, S.D., and L.D. Brandeis, op cit, p. 193.
[6] Prosser, W.L. (1960). Privacy. *California Law Review*, 48(3), 383-423; Allen, A.L. (2011). *Privacy Law and Society, 2nd ed*. St. Paul, MN: West/Thomson, p. 40.
[7] Prosser, W.L., op cit; Privacilla.org. (2002). The Privacy Torts: How U.S. State Law Quietly Leads the Way in Privacy Protection. *Privacilla.org*. Retrieved November 11, 2014 from http://www.privacilla.org/releases/Torts_Report.pdf; Restatement (Second) of Torts § 652 (1977).
[8] Ibid.
[9] Ibid.
[10] Ibid.
[11] Ibid.
[12] Restatement (Second) of Torts, op cit; Privacilla.org, op cit; Allen, A.L., (2011), *Privacy Law and Society, 2nd ed*., op cit, p. 40.
[13] Allen, A.L., (2011), *Privacy Law and Society, 2nd ed*., op cit, p. 40.

of action have served as the basis of invasion of privacy law suits throughout the 20th and early 21st centuries.[14]

Case law and legislative action around the right to privacy began to accumulate in the early 20th century and especially in the 1960s and 1970s—an era of major social change coupled with important technological innovation. Increasing use of espionage and surveillance during the Cold War, the Vietnam conflict, and the civil rights era caused many to question whether there were limits on society's right to know certain information.[15] With the advent of computers in the 1970s came concerns about the collection and privacy of information.[16]

In the 1960s and 1970s, the United States Supreme Court decided a number of fundamental privacy cases and set important precedent, including questions about physical privacy (i.e., lawful search and seizure) and decisional privacy (i.e., access to birth control and reproductive choice).[17] In addition, Congress enacted a number of laws designed to protect privacy in particular areas. For example, concerns about computers and the electronic collection of personal information prompted the Privacy Act of 1974 and the Family Education and Right to Privacy Act of 1974, among others.[18] (See section IV.D.2, *Legal Notions of Privacy – U.S. Statutory Protection* for more detail.)

B. Privacy and Related Concepts

There is no consensus definition of privacy. Privacy has referred to a person's ability to seclude or conceal themselves; the lack of access to a person's emotions, beliefs, mental states, habits, and past conduct; and the anonymizing of data, facts, or conversations.[19] Privacy is sometimes thought of as access to and control over certain personal information. A person has privacy with respect to a particular piece of information if others cannot access that information, or if the individual maintains control over that information.[20] Many also explain privacy's value in terms

[14] Prosser, W.L., op cit; Allen, A.L., (2011), *Privacy Law and Society, 2nd ed*., op cit, pp. 11-237.
[15] Allen, A. (2003). Privacy. In H. LaFollette. (Ed.). *The Oxford Handbook of Practical Ethics* (pp. 485-513). New York, NY: Oxford University Press.
[16] Ibid.
[17] Ibid.
[18] Ibid.
[19] Allen, A.L. (2011). *Unpopular Privacy: What Must We Hide?* New York, NY: Oxford University Press, p. 4; Allen, A.L. (1988). *Uneasy Access: Privacy for Women in a Free Society*. Totowa, NJ: Rowman & Littlefield, pp. 1-34.
[20] Parent, W.A. (1983). Privacy, morality, and the law. *Philosophy & Public Affairs*, 12(4), 269-288; Gavison, R. (1980). Privacy and the limits of law. *The Yale Law Journal*, 89(3), 421-471; Allen, A.L. (1988), op cit, p. 15; Powers, M. (1996). A cognitive access definition of privacy. *Law and Philosophy*, 15(4), 369–386; Beardsley, E. (1971). Privacy, Autonomy, and Selective Disclosure. In J.R. Pennock and J.W Chapman. (Eds.). *NOMOS XIII: Privacy* (pp. 65-70). New York, NY: Atherton Press; Westin, A.F. (1967). *Privacy and Freedom*. New York, NY: Athenum, p. 7; Moore, A.D. (2010). *Privacy Rights: Moral and Legal Foundations*. University Park, PA: The Pennsylvania State University Press; Rachels, J. (1975). Why privacy is important. *Philosophy & Public Affairs*, 4(4), 323–333.

of individual autonomy. Under these views, privacy is important either as an object of autonomous choice or as a condition of exercising autonomy.[21]

The umbrella term "privacy" includes different types of privacy. For example, informational privacy governs the collection, use, and sharing of information or data. Physical privacy pertains to observing, concealing, and touching the human body. Spatial, geographical, and locational privacy refer to Global Positioning System (GPS) and beeper technologies, which can track and divulge an individual's whereabouts. Associational privacy relates to affiliation with groups of people. Decisional privacy gives rise to independent decision-making. Intellectual privacy relates to interests in freedom of thought, conscience, and access to knowledge.[22]

Notions of privacy are often used in conjunction with or in contrast to notions such as confidentiality, secrecy, information security, decisional autonomy, and freedom from unwanted intrusion.[23] Confidentiality generally means restricting access to specific information only to those authorized to receive it.[24] Disclosure of health information, for example, is often limited by custom to close family and friends and by law to health practitioners, insurers, and professional researchers.[25] Anonymity includes limiting access to personally identifiable information through intentionally disguising or removing identifiers such as an individual's name, address, or social security number.[26] Data protection refers to measures implemented to prevent disclosure of confidential or anonymous information; for information stored electronically, computer passwords and encryption are useful tools to protect data.[27]

C. Guiding Ethical Principles

In its work on privacy, the Bioethics Commission considered a number of applicable ethical principles.

The first principle, respect for persons, recognizes that individuals are autonomous agents who are capable of deciding for themselves what they value and how and when to act on those values.[28] Respect for persons requires giving great "weight to autonomous persons' considered opinions and choices while refraining from obstructing their actions unless they are clearly

[21] Allen, A.L. (1988), op cit, p. 43.
[22] PCSBI, (2012, October), op cit, p. 40; Allen, A.L., (2011), *Privacy Law and Society, 2nd ed*., op cit, pp. 4-6.
[23] DeCew, J.W. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca, NY: Cornell University Press, pp. 46-80; Allen, A.L. (1988), op cit, pp. 5-11; Solove, D.J. (2002). Conceptualizing privacy. *California Law Review*, 90(4), 1087-1156.
[24] PCSBI, (2012, October), op cit, p. 39.
[25] PCSBI, (2012, October), op cit, p. 39.
[26] PCSBI, (2012, October), op cit, p. 39.
[27] PCSBI, (2012, October), op cit, p. 39.
[28] PCSBI, (2012, October), op cit, p. 45.

detrimental to others."[29] Privacy—and the right to make important decisions without outside interference—is an important condition for persons exercising autonomy.

The second principle, "public beneficence, requires both that public benefits be secured and that public harms be minimized."[30] "Public beneficence gives rise to a societal and governmental duty to promote individual activities and institutional practices… that have great potential to improve the public's wellbeing."[31] There is a corresponding duty to minimize the societal and individual harms that can result from scientific and technical advances. Privacy protections are one way of minimizing the harms, such as the unauthorized disclosure of private health information, that can befall those receiving clinical care or participating in research.

The principles of respect for persons and public beneficence can come into tension. Certain societal advances require access to information that individuals would prefer to keep private. Medical advances from whole genome sequencing, for example, depend on people being willing to share their whole genome sequence data and information. Public health practitioners need access to otherwise private medical information to help prevent the spread of infectious diseases. Reconciling the principles of respect for persons and public beneficence can be challenging and requires consideration of the particular facts and circumstances at issue.

The ethical principle of responsible stewardship calls for governments and societies to proceed prudently in promoting science and technology that can improve human welfare but can also cause harm, and to recognize the importance of citizens and their representatives acting collectively for the betterment of all, especially those who cannot represent themselves.[32] Groups requiring additional protection can include children, individuals with impaired capacity to consent, or individuals that might be unaware of risks of engaging in particular acts. Additional privacy protections for those unable to understand fully the consequences of their actions are afforded in some circumstances.

A fourth principle is intellectual freedom and responsibility. Intellectual freedom grants scientists, acting responsibly, the right to use their creative abilities to advance science and the public good. Intellectual responsibility calls upon responsible parties to adhere to ethical ideals that include avoiding harm to others and abiding by applicable policies, rules, and regulations.[33] As a corollary, the principle of regulatory parsimony calls for "only as much oversight as is truly

[29] PCSBI, (2012, October), op cit, p. 45; National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research*. Washington, DC: Department of Health, Education, and Welfare, DHEW Publication OS 78-0012. Retrieved October 6, 2014 from http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html.
[30] PCSBI, (2012, October), op cit, p. 36.
[31] PCSBI, (2012, October), op cit, p. 35.
[32] PCSBI, (2010, December). *New Directions: The Ethics of Synthetic Biology and Emerging Technologies*. Washington, DC: PCSBI, p. 25.
[33] PCSBI, (2012, October), op cit, p. 29.

necessary to ensure justice, fairness, security, and safety while pursing the public good."[34] In the context of privacy, this means acting in accordance with ethical norms and adhering to legal restrictions on what can be done with private information. Those passing laws that protect privacy should do so mindful of the principle of regulatory parsimony.

Democratic deliberation, an approach to collaborative decision making, embraces respectful debate of opposing views and active participation by citizens. Democratic deliberation warrants engaging the public and fostering dialogue among various stakeholders concerned about an issue.[35] When grappling with new privacy protections or considering the privacy issues raised by novel and emerging technologies, each approach to privacy protection should be publically debated consistent with the principle of democratic deliberation.

Finally, the principle of justice and fairness relates to the distribution of benefits and burdens across society, ensuring that the unavoidable burdens of technological advances do not fall disproportionately on a particular individual or group, and that the benefits are widely and equitably distributed.[36] Those who have access to private information should take special care, including protecting against unauthorized disclosure, to ensure that burdens do not fall disproportionately on any particular individual or group.

D. Legal Notions of Privacy

1. U.S. Case Law

In the United States, explicit discussion and use of the term "the right to privacy" is thought to have originated in an article published by in 1890 by Samuel Warren and future Supreme Court Justice Louis Brandeis. Their article, "The Right to Privacy," argued that U.S. law should recognize a privacy interest in one's personal life. Despite the article's advocacy for and recognition of the importance of safeguarding the private sphere, it wasn't until the mid-1960s that the U.S. Supreme Court articulated a constitutional right to privacy.

The Supreme Court has recognized a right to privacy found in the "penumbras" or "emanations" of other explicitly enumerated rights (i.e., implied by other rights, but not explicitly stated in the Constitution). In particular, the right to privacy is thought to arise from the First Amendment, guaranteeing freedom of speech, as well as freedom of religious, political, and personal association, and related forms of anonymity; the Third Amendment, granting freedom from government appropriation of one's home; the Fourth Amendment, granting freedom from unreasonable search and seizure of one's body and property; the Fifth Amendment, granting freedom from compulsory self-incrimination; the Eighth Amendment, granting freedom from cruel and unusual punishment, including unnecessarily extreme deprivations of privacy; and the

[34] PCSBI, (2012, October), op cit, p. 29.
[35] PCSBI, (2012, October), op cit, p. 30.
[36] PCSBI, (2012, October), op cit, p. 30.

Ninth Amendment, granting other personal freedoms.[37] The Supreme Court has also recognized privacy rights to decisions affecting personal life free from substantial government interference under the 14th Amendment.

The body of privacy case law, beginning in 1965 with *Griswold v. Connecticut*, addresses two distinct privacy interests.[38] First, a line of cases addresses a privacy and autonomy right to make certain kinds of decisions—including decisions about whom to marry and with whom to procreate. A second line of cases addresses the privacy interest in avoiding disclosure of personal matters, including in violation of the Fourth Amendment's protection from unreasonable search and seizure.

The Supreme Court's first major case to address an individual's right to privacy in the medical sphere was *Griswold v. Connecticut*.[39] In *Griswold*, the Supreme Court considered a Connecticut state law that prohibited the use of contraception. By a vote of 7 to 2, the Supreme Court invalidated the Connecticut law holding that it interfered with the right to marital privacy. Seven years later, in *Eisenstadt v. Baird*, the Supreme Court extended its holding in *Griswold*—that married individuals have the right to make decisions about contraception free from unwarranted government intrusion—to unmarried individuals.[40] In *Eisenstadt*, the Supreme Court reached its decision on the basis of the Fourteenth Amendment's Equal Protection clause, recognizing that the law as written resulted in irrational discrimination between married and unmarried individuals.

In *Katz v. United States*, decided in 1967, the Supreme Court addressed concerns about a second privacy interest—the interest in avoiding disclosure of personal matters.[41] *Katz* involved the FBI recording conversations using an electronic device attached to the exterior of a public phone booth. During conversations, Charles Katz used the phone booth to transmit information about illegal gambling. The Fourth Amendment protects against unreasonable search and seizure. The question before the Supreme Court was whether the FBI's action was a search and whether it was reasonable. The Court held that the Fourth Amendment protected all areas where an individual had a reasonable expectation of privacy and that the FBI's actions violated the privacy on which Charles Katz justifiably relied.

In 1973, the Supreme Court considered the issue of a woman's right to terminate a pregnancy in the case *Roe v. Wade*.[42] At issue was a Texas state law that criminalized helping a woman obtain an abortion. The Supreme Court held that "the fundamental right to privacy, grounded in the

[37] PCSBI, (2012, October), op cit, p. 37.
[38] *Griswold v. Connecticut*, 381 U.S. 479 (1965).
[39] Ibid.
[40] *Eisenstadt v. Baird*, 405 U.S. 438 (1972).
[41] *Katz v. United States*, 389 U.S. 347 (1967).
[42] *Roe v. Wade*, 410 U.S. 113 (1973).

fourteenth amendment's concept of personal liberty, encompasses a woman's decision" to terminate a pregnancy.

Although the Supreme Court made important progress in delineating a constitutional right to privacy throughout the 1960s and 1970s, the Supreme Court still faces—and will continue to face—important privacy questions. With regard to the privacy interest in making personal and fundamental decisions, in the 2003 case *Lawrence v. Texas*, the Supreme Court struck down a Texas state law that criminalized certain adult same-sex intimate sexual acts.[43] The majority opinion struck down the statute as an unjustified "intrusion into the personal and private life of the individual" and found that the Texas statute invaded "the most private human conduct, sexual behavior, and in the most private of places, the home."[44]

More recently, in *United States v. Jones*, decided in 2012, the Supreme Court faced the question of whether a GPS device installed on a car to monitor the car's movement should be considered a search for purposes of the Fourth Amendment.[45] Although the Supreme Court unanimously held that the installation of a GPS device was a Fourth Amendment search, the Court was split as to the rationale.[46]

2. U.S. Statutory Protection

From early U.S. history, the U.S. government has collected personally identifiable information about its citizens. Through information gathering processes such as the census and tax collection, individuals submit information to the government that they generally otherwise would keep private.

Although initially unprotected, this information has become subject to increased privacy protections over time. For example, identifiable census information cannot be published for use for any purpose other than "the statistical purposes for which it is supplied."[47] Anyone who communicates or publishes any census information can be subject to up to five years in prison, $250,000 in fines, or both.[48] Only "a restricted number of authorized people have access to private information," and everyone who works with private information "is sworn for life to uphold the law."[49] The Internal Revenue Service similarly has an extensive body of law designed

[43] *Lawrence v. Texas*, 539 U.S. 558 (2003).
[44] *Lawrence v. Texas*, 539 U.S. 558, 578, 567 (2003).
[45] *United States v. Jones*, 565 U.S. __, 132 S. Ct. 945 (2012).
[46] A five Justice majority concluded that the police action constituted a search because of the physical intrusion, whereas a four Justice minority concluded that the GPS monitoring constituted a violation of Jones' reasonable expectation of privacy. The Supreme Court has not yet answered the question of whether GPS tracking without a physical intrusion—such as by collecting GPS data from mobile phone operators—would similarly count as a Fourth Amendment search. *United States v. Jones*, 565 U.S. __, 132 S. Ct. 945 (2012).
[47] *Census*, 13 U.S.C. § 9.
[48] United States Census Bureau. (n.d.). American Community Survey: How We Protect Your Privacy [Webpage]. Retrieved October 6, 2014 from http://www.census.gov/acs/www/about_the_survey/we_protect_your_privacy/.
[49] United States Census Bureau. (n.d.). Data Protection and Privacy Policy: Our Privacy Principles [Webpage]. Retrieved October 6, 2014 from http://www.census.gov/privacy/data_protection/our_privacy_principles.html. Basic

to maintain the confidentiality of tax return data.[50] Unauthorized disclosure can lead to criminal charges against the federal officer or employee and to a civil lawsuit for monetary damages brought by the wronged party.[51]

The U.S. government also has promulgated a number of privacy laws that provide protection for specific areas. These laws, discussed below in more detail, generally comport with "fair information practice" principles that require that: 1) there is no personal data record-keeping systems for which the very existence is secret; 2) individuals must be able to find out what personal information about them is in a record and how it is used; 3) individuals must be able to prevent information obtained for one purpose from being used for other purposes without consent; 4) individuals must be able to correct or amend a record of identifiable information; and 5) any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.[52]

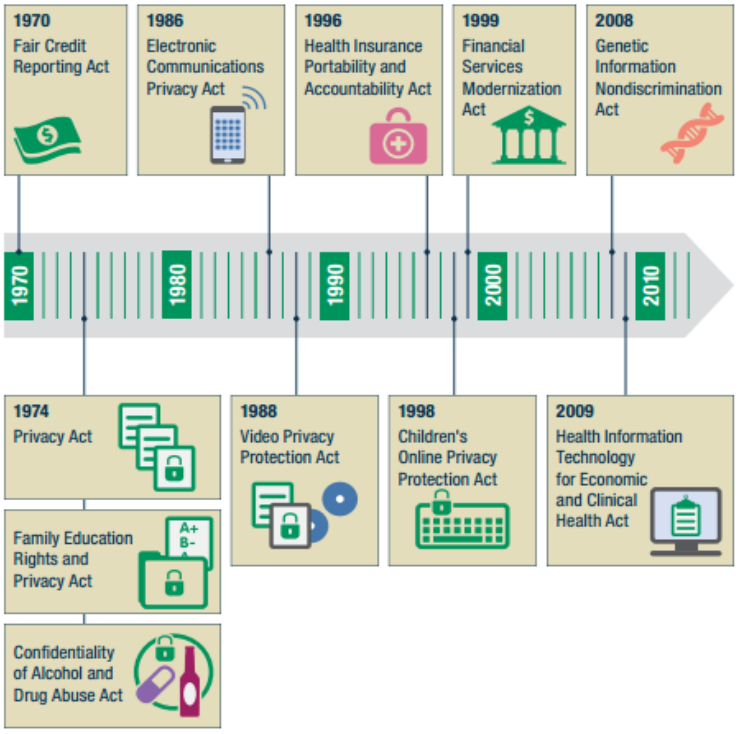
The graphic below provides a timeline of some of the sectoral statutory privacy protections that have been enacted in the United States.

census data is released publically 72 years after it is collected. United States Census Bureau. (n.d.). History: The "72-Year Rule" [Webpage]. Retrieved October 6, 2014 from https://www.census.gov/history/www/genealogy/decennial_census_records/the_72_year_rule_1.html.

[50] Internal Revenue Service. (2013). Internal Revenue Manual (IRM) 11.3.14, Privacy Act General Provisions: 11.3.14.3 Limitations. Retrieved October 6, 2014 from http://www.irs.gov/irm/part11/irm_11-003-014.html.

[51] *Internal Revenue Code*, 26 U.S.C. § 7213(a)(1); *Internal Revenue Code*, 26 U.S.C. § 7431(c).

[52] Secretary's Advisory Committee on Automated Personal Data Systems. (1973). *Records, Computers and the Rights of Citizens* (DHEW Publication No. (OS) 73-64). Washington, DC: Department of Health, Education, and Welfare (DHEW). Retrieved October 6, 2014 from http://www.justice.gov/sites/default/files/opcl/docs/rec-com-rights.pdf.



Source: Presidential Commission for the Study of Bioethical Issues (PCSBI). (2012, October). *Privacy and Progress in Whole Genome Sequencing*. Washington, DC: PCSBI, p. 61.

The specific privacy statutes described below illustrate the sectoral, segmented approach to privacy that the United States has taken.

Fair Credit Reporting Act (1970)

The Fair Credit Reporting Act, the first modern American privacy law, regulates the collection, dissemination, and use of consumer information.[53] The Act delineates the particular circumstances in which a consumer report may be transmitted to another party, the types of information that cannot be included in any credit report, the circumstances in which a person must be notified that a report is being prepared about them, and the procedures that must be implemented to prevent unauthorized disclosures.[54] The Act also authorizes consumers to request all information in their file, the sources of the information, and who requested the information subject to certain enumerated exceptions.[55] Consumers are allowed to dispute the accuracy of

[53] *Fair Credit Reporting Act*, 15 U.S.C. § 1681 et seq.
[54] Ibid.
[55] *Fair Credit Reporting Act*, 15 U.S.C. § 1681g.

any information contained within the file, and are entitled to bring a civil lawsuit in the event of an unauthorized disclosure.[56]

Privacy Act (1974)

The Privacy Act, enacted in response to concerns about the impact of burgeoning computerized databases on individuals' privacy rights, regulates the collection, maintenance, use and disclosure of personal information by federal agencies.[57] The Privacy Act creates four procedural and substantive rights in personal data. First, the Act requires that government agencies show an individual any records kept on him or her. Second, the Act requires agencies to follow "fair information practices." Third, the Act places restrictions on how agencies can share data. And fourth, the Act lets individuals sue the government for unauthorized disclosures.[58]

A second statute pertaining to the government's collection of information, the Freedom of Information Act (FOIA), gives individuals the right to access information from the federal government.[59] The government does not have to disclose information if, however, the requested information falls within one of nine exceptions, including an exception for disclosing documents for which disclosure "would constitute a clearly unwarranted invasion of personal privacy."[60] As interpreted, if such an exemption to a FOIA request applies, the Privacy Act makes withholding the requested document mandatory; if no exemption applies such that FOIA requires disclosure, the Privacy Act will not prevent disclosure of the document.[61]

Family Educational Rights and Privacy Act (1974)

The Family Educational Rights and Privacy Act governs access to, and disclosure of, educational records.[62] The Act gives parents access to their child's student records, a process whereby they can seek to have their child's record amended, and control over disclosure of the student's record subject to certain exceptions. Once a student turns 18 years old, the student generally must provide consent before his or her record is released.

Confidentiality of Alcohol and Drug Abuse Act (1974)

In response to concerns that stigma associated with substance abuse and fear of prosecution deterred people from entering treatment, Congress enacted the Confidentiality of Alcohol and Drug Abuse Act which grants those seeking treatment for substance abuse the right to keep

[56] *Fair Credit Reporting Act*, 15 U.S.C. § 1681i.
[57] *Privacy Act*, 5 U.S.C. § 552a.
[58] Electronic Privacy Information Center. (n.d.). The Privacy Act of 1974 [Webpage]. Retrieved October 6, 2014 from http://epic.org/privacy/1974act/.
[59] *The Freedom of Information Act*, 5 U.S.C. § 552.
[60] *The Freedom of Information Act*, 5 U.S.C. § 552(b)(6).
[61] News-Press v. DHS, 489 F.3d 1173, 1189 (11th Cir. 2007).
[62] *Family Educational Rights and Privacy Act*, 20 U.S.C. § 1232g.

aspects of the related records confidential.[63] In general, records relating to substance abuse treatment that is conducted by a federal program shall be kept confidential.[64] Records may be disclosed with the patient's written consent.[65] Records may be disclosed even without the patient's consent if there is a bona fide medical emergency; for scientific research or audit purposes, if the information is not identifiable; and in response to a specifically crafted court order.[66]

Electronic Communications Privacy Act (1986)

The Electronic Communications Privacy Act is intended to provide safeguards in addition to those provided by the Fourth Amendment. The Electronic Communications Privacy Act protects against unauthorized access to transmissions of electronic data by private persons/companies and the government.[67] Title I of the Act provides stringent requirements for search warrants for electronic communications while in transit. Title II of the Act protects communications held in electronic storage (e.g., messages stored on computers). Title III prohibits the use, without a court order, of certain devices to record particular types of signaling information used in the transmission of electronic communications. The Electronic Communications Privacy Act has been criticized, however, as offering out-of-date privacy protections; for example, email stored on a third party's server for more than 180 days is considered abandoned and can be accessed by law enforcement without a warrant.

Video Privacy Protection Act (1988)

The Video Privacy Protection Act of 1988 "stands as one of the strongest protections of consumer privacy against a specific form of data collection."[68] The Act forbids disclosure of personally identifiable information about video rentals to anyone besides the consumer except in circumstances in which the consumer provides express written consent, or in specifically enumerated circumstances.[69] One whose information has been disclosed in violation of the Act may bring a civil lawsuit for actual damages, punitive damages, and attorneys' fees.[70] Video

[63] U.S. Department of Health and Human Services (HHS). (2004). The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs. June. Retrieved October 6, 2014 from http://www.nj.gov/humanservices/das/information/SAMHSA-Pt2-HIPAA.pdf; *Confidentiality of Alcohol and Drug Abuse Act*, 42 U.S.C. § 290dd-2.
[64] *Confidentiality of Alcohol and Drug Abuse Act*, 42 U.S.C. § 290dd-2(a).
[65] *Confidentiality of Alcohol and Drug Abuse Act*, 42 U.S.C. § 290dd-2(b)(1).
[66] *Confidentiality of Alcohol and Drug Abuse Act*, 42 U.S.C. § 290dd-2(b)(2).
[67] *Electronic Communications Privacy Act*, 18 U.S.C. § 2510-22.
[68] *Video Privacy Act*, 18 U.S.C. § 2710; Electronic Privacy Information Center. (n.d.). Video Privacy Protection Act [Webpage]. Retrieved October 6, 2014 from http://epic.org/privacy/vppa/.
[69] *Video Privacy Act*, 18 U.S.C. § 2710(b)(2)(B).
[70] *Video Privacy Act*, 18 U.S.C. § 2710(c).

rental records must be destroyed no later than one year after a video rental account has been terminated.[71] States are free to enact broader privacy protections for video rental records.[72]

Health Insurance Portability and Accountability Act (1996)

The Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 is the primary law protecting the privacy of individually identifiable health information as collected by covered entities (e.g., health maintenance organizations, health care clearinghouses, and certain health care providers). HIPAA is discussed in more detail in the section IV.E. *Privacy of Health Information*.

Children's Online Privacy Protection Act (1998)

The Children's Online Privacy Protection Act was enacted to safeguard children under the age of 13 from the online collection and use of private data. This law sets forth what a website operator must include in its privacy policy, when and how the consent of the parent or guardian must be obtained, and the responsibility that website operators have to protect a child's privacy and safety online.[73]

Gramm-Leach-Bliley Act (1999) [Title V of the Financial Services Modernization Act]

The Gramm-Leach-Bliley Act restricts the ability of financial institutions to use and disseminate private financial data.[74] As a result of this law, financial institutions must provide all consumers with a privacy notice when the relationship is established, and at yearly intervals thereafter. The notice must explain what information about the consumer is collected, with whom that information is shared and how it is used, the protections that are being offered, and the consumer rights to prevent information from being shared.

Genetic Information Nondiscrimination Act (2008)

The Genetic Information Nondiscrimination Act (GINA) protects against genetic discrimination in the health insurance market and employment decisions such as hiring, firing, job assignments, and promotions. GINA is discussed in more detail in the section IV.E. *Privacy of Health Information*.

Health Information Technology for Economic and Clinical Health Act (2009)

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted to promote the adoption and meaningful use of health information technology, including

[71] *Video Privacy Act*, 18 U.S.C. § 2710(e).
[72] *Video Privacy Act*, 18 U.S.C. § 2710(f).
[73] *Children's Online Privacy Protection Act*, 15 U.S.C. §§ 6501–6506.
[74] *Gramm-Leach-Bliley Act*, Pub. L. 106-102, 113 Stat. 1338. The Act also permits commercial banks, investment banks, securities firms, and insurance companies to coordinate.

the privacy and security concerns associated with electronic transmission of health information.[75] HITECH is discussed in more detail in the section IV.E. *Privacy of Health Information*.

3. The European Approach

In contrast to the sectoral, context-specific approach to privacy employed in the United States, Europe has taken a more expansive approach. In Europe, privacy is considered a fundamental human right. Privacy is protected under Article 8 of the European Convention on Human Rights, which provides for a "right to respect for private and family life."[76] This privacy right has been interpreted broadly in European case law. Privacy is also protected under Directive 95/46/EC, the "Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," which regulates the processing of citizens' personal data.[77]

The difference between the U.S. and European approaches gives rise to important consequences. As a paradigmatic example of the two different approaches, in 1985, a gay man successfully sued to prevent a French publication from publishing a photo of him at a gay pride parade in Paris.[78] Around the same time in the United States, the California Supreme Court upheld the rights of journalists to disclose the sexuality of Oliver Sipple—a man who helped foil an assassination attempt on then-President Gerald Ford—because he was declared a public figure who thereby surrendered many of his privacy rights. Sipple had not yet disclosed his sexual orientation to his family, and ultimately committed suicide.[79]

Although the United States provides statutory protection for some health information, the protections are less encompassing than those in Europe. Europeans have broad protection in the event their health information is disclosed in an unauthorized manner. By contrast, Americans are protected if their health information is disclosed in contravention of a statute (e.g., if disclosed in an unauthorized manner by a covered entity under HIPAA), but do not have the

[75] U.S. Department of Health and Human Services (HHS). (n.d.). HITECH Act enforcement interim final rule [Webpage]. Retrieved October 6, 2014 from http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html.
[76] European Court of Human Rights. (2010). European Convention on Human Rights - Article 8, p. 10. Retrieved October 6, 2014 from http://www.echr.coe.int/Documents/Convention_ENG.pdf.
[77] This directive does not consider aspects including globalization or evolving technologies such as social networks or cloud computing. Accordingly, a proposal for new regulation was released on January 25, 2012. The EU's European Council intends for a new regulation to be adopted in late 2014, with a plan to take effect over a two-year transition period. European Commission (2011). Protection of Personal Data [Webpage]. Retrieved October 6, 2014 from http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm; European Commission. (2014). Data Protection Day 2014: Full Speed on EU Data Protection Reform [Press release]. Retrieved October 6, 2014 from http://europa.eu/rapid/press-release_MEMO-14-60_en.htm; European Commission. (2014). Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote [Press release]. Retrieved October 6, 2014 from http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.
[78] Sullivan, B. (2006, October 19). 'La difference' is stark in EU, U.S. privacy laws. *NBC News*. Retrieved October 6, 2014 from http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/#.VBHd3PmtaMA.
[79] Ibid.

same protections if that same information was disclosed on a website hosted by a private company.[80]

E. Privacy of Health Information

Health information raises discrete privacy concerns because of the sensitive nature of the information. There is concern that inadequate protections of health information could lead people to engage in privacy-protecting behaviors, such as avoiding health care, lying to health care providers, or not participating in research.

In 1996, the U.S. government enacted HIPAA, a law governing several aspects of health insurance. HIPAA required the creation of a Privacy Rule for the protection of identifiable health information. HIPAA's Privacy Rule, finalized in August 2002, sets forth the circumstances in which an individual's protected health information may be used or disclosed by a covered entity (a health plan, a health care clearinghouse, or a health care provider).[81] For example, a covered entity *may* disclose protected health information without consent in specifically enumerated circumstances, including for purposes related to public health. A covered entity that discloses protected health information, however, must try to disclose only the minimum necessary to achieve its purpose.[82] The Privacy Rule also provides a way in which information can be used if de-identified (i.e., stripped of personally identifying information). In particular, the Privacy Rule lists 18 identifiers—including name, address, and social security number—that must be removed from health information for it to be considered "de-identified." Although the Privacy Rule protects the privacy of some health information in certain circumstances, the Privacy Rule does not provide comprehensive privacy protection. Importantly, HIPAA does not provide a private right of action; that is, those who believe that their rights have been violated cannot sue under HIPAA. There have been, however, a number of fines levied by the U.S. Department of Health and Human Services (HHS) under HIPAA. In May and June 2014, for example, HHS settled a data breach case for $4.8 million and a medical records dumping case for $800,000.[83]

HITECH, intended to facilitate the transition to electronic medical records, updated and revised HIPAA and extended its privacy protections slightly. HITECH adds business associates of covered entities to the list of those who can be subject to liability for disclosure of protected health information. It also strengthens the accounting requirements for the protection of health information, and imposes new notification requirements for covered entities to comply with

[80] Ibid.
[81] *HIPAA Privacy Rule*, 45 C.F.R. § 164.501.
[82] *HIPAA Privacy Rule*, 45 C.F.R. § 164.502(b).
[83] U.S. Department of Health and Human Services (HHS). (n.d.). Health Information Privacy: Case Examples and Resolution Agreements [Webpage]. Retrieved October 29, 2014 from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/.

when a breach has occurred.[84] Most academic institutions and federal agencies also follow the Common Rule, a federal regulation governing federally supported human research in the United States. The Common Rule requires, among other things, that risks to participants—including privacy risks—be minimized.[85]

Genomic privacy receives some additional protection at both the federal and state levels. In 2008, Congress passed GINA, which prevents genetic discrimination in the health insurance market (Title I) and employment decisions such as hiring, firing, job assignments, and promotions (Title II).[86] GINA does not, however, protect against discrimination in the context of life, disability, or long-term care insurance. GINA also expanded HIPAA privacy protections by applying prohibitions against genetic discrimination to all health insurers.[87] GINA is an anti-discrimination law; it does not provide comprehensive privacy protections.

About half of all U.S. states have policies governing genetic privacy, although there is variation in what protections states afford their citizens. Slightly fewer than half of all U.S. states have laws providing additional protection against discrimination in aspects of life, long-term care, or disability insurance not present in GINA.[88] Some states protect against the improper collection of genetic material without consent.[89] Others protect against the improper disclosure of genetic information.[90] Still others protect against improper retention of genetic information without consent.[91]

Although medical privacy broadly, and genetic privacy in particular, are afforded some additional protections, the level of protection under the patchwork of laws is less absolute than under Europe's more expansive approach.

[84] *Health Information Technology for Economic and Clinical Health* (*HITECH*), 42 U.S.C. § 300jj; Office of the National Coordinator for Health Information Technology (ONC). (n.d.). About ONC [Webpage]. Retrieved October 6, 2014 from http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__onc/1200.
[85] *Protection of Human Subjects*, *HHS*. 45 C.F.R. § 46.
[86] *Genetic Information Nondiscrimination Act* (*GINA*), 122 Stat. 881-922.
[87] *Health Insurance Portability and Accountability Act* (*HIPAA*), 29 U.S.C. §§ 1181-82; *HIPAA*, 42 U.S.C. §§ 300gg-41.
[88] See Presidential Commission for the Study of Bioethical Issues (PCSBI). (2012, October). *Privacy and Progress in Whole Genome Sequencing*, Appendix IV: U.S. State Genetic Laws. Washington, DC: PCSBI, pp. 121-124; National Human Genome Research Institute. (2014). Genome Statute and Legislation Database. Retrieved October 6, 2014 from http://www.genome.gov/PolicyEthics/LegDatabase/pubsearch.cfm.
[89] See e.g., Del. Code Ann. §§ 12.2.1220 to 12.2.1227.
[90] See e.g., Ariz. Rev. Stat. Ann. § 12-2801-4, § 20-448.02.
[91] See e.g., Nev. Rev. Stat. Ann. § 613.345, 629.101-629.201.

F. Challenges to De-identification

De-identifying data by removing specific identifiers, such as name and social security number, might not be sufficient to secure anonymity.[92] For example, individuals might be re-identified by linking or matching their de-identified health information to other databases. De-identified information could also contain unique and unusual information which renders it particularly easy to re-identify. Alternatively, those with access to the data might possess knowledge that makes it easier to re-identify an individual.[93] Given these challenges to de-identification, individuals cannot always assume that their anonymity is protected even if specific personal identifiers have been removed.

V. Discussion Questions

The following questions are based on the information provided in the "Background" section and are intended to reinforce important aspects of privacy that are highlighted in this module. Important points are noted with each question to help the instructor guide a group discussion. The "Additional Resources" section will be helpful in answering these questions.

1. What is privacy?

Starting points for discussion:

a. There is no consensus definition of privacy.

b. Privacy can refer to the ability of a person to seclude or conceal themselves; the lack of access to a person's emotions, beliefs, mental states, habits, and past conduct; and the keeping secret or anonymizing of data, facts, or conversations.

c. Privacy also can denote the absence of substantial government or other outside interference with an individual's decisions and choices, a type of decisional autonomy.

d. Privacy is sometimes thought of as access to and control over certain pieces of information. A person has privacy with regard to a particular piece of information if others cannot access that piece of information, or if the individual maintains control over that information.

[92] Sweeney, L. (1997). Weaving technology and policy together to maintain confidentiality. *Journal of Law, Medicine & Ethics*, 25(2-3), 98-110.
[93] Ibid.

2. What is the value of privacy?

Starting points for discussion:

a. Respect for persons recognizes that individuals are autonomous agents who are capable of deciding for themselves what they value, and how and when to act on those values. Many explain the value of privacy in terms of individual liberty. These views maintain that privacy is important either as an object of autonomous choice or as a condition of independence. The complete absence of government regulation of families and personal matters is not, however, the objective as most people support laws against incest or sex with children.

b. Privacy protections for important information allow individuals to decide when, how, and with whom to share information are therefore important in exercising autonomy.

3. How has U.S. case law helped establish the right to privacy?

Starting points for discussion:

a. *Griswold v. Connecticut* (1965) prohibited the criminalization of access to birth control for married couples. *Eisenstadt v. Baird* (1972) extended the right to use contraception to unmarried individuals.

b. *Katz v. United States* (1967) established that warrantless wiretapping violated the Fourth Amendment right to protection from unreasonable search and seizure.

c. *Roe v. Wade* (1973) established a fundamental privacy interest in the choice to terminate a pregnancy, grounded in the Fourteenth Amendment's concept of personal liberty.

d. *Lawrence v. Texas* (2003) established the right for adults to participate in private, consensual sexual conduct, striking down state-level laws.

4. How does the Health Insurance Portability and Accountability Act (HIPAA) protect personal health information? What are its limitations?

Starting points for discussion:

a. HIPAA's Privacy Rule, finalized in 2002, sets forth policies, procedures, and guidelines for maintaining the privacy and security of personally identifiable health information in certain circumstances.

b. The HIPAA-mandated Privacy Rule was finalized in 2002. The Privacy Rule defines the circumstances in which an individual's protected health information—including any identifiable information—may be used or disclosed by a covered entity. HIPAA does not, however, provide a private right of action; that is, those who believe that their rights have been violated cannot sue under HIPAA.

c. A covered entity must disclose an individual's protected health information to him or her when requested specifically, and to HHS in the event of a compliance investigation or enforcement action. A covered entity may disclose protected health information without consent in specifically enumerated circumstances, including for purposes related to treatment, payment, public health, and health care operations. A covered entity that discloses protected health information, however, must disclose only the minimum necessary to achieve its purpose. There are no restrictions on the use or disclosure of de-identified health information—information that has been separated from details identifying the individual from whom they were derived.

VI. Exercises

Exercise A. *Fair information practices are a basic set of obligations by which organizations that process personal information should abide.*

The following reference discusses fair information practices:

> Schwartz, P.M. (2009). Preemption and privacy. *The Yale Law Journal*, 118, 902-947.
>
> Fair information practices include "(1) limits on information use; (2) limits on data collection, also termed data minimization; (3) limits on disclosure of personal information; (4) collection and use only of information that is accurate, relevant, and up-to-date (data quality principle); (5) notice, access, and correction rights for the individual; (6) the creation of processing systems that the concerned individual can understand (transparent processing systems); and (7) security for personal data" (p. 908).

1. **How do the fair information practices protect individual privacy interests?**

2. **What is the European Union's (EU) "right to be forgotten" rule? What are its limitations?**

The following references provide useful information:

European Commission. (n.d.). Factsheet on the "Right to be Forgotten" ruling (C-131/12). Retrieved October 6, 2014 from http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

Lee, D. (2014, May 13). What is the 'right to be forgotten'? *BBC*. Retrieved October 6, 2014 from http://www.bbc.com/news/technology-27394751.

3. **How does the EU's "right to be forgotten" rule comply with fair information practices?**

4. **Statutes that implement fair information practices generally apply to fairly narrow subject matter. Read the Confidentiality of Alcohol and Drug Abuse Act and describe how the statute exemplifies the principles of fair information practices.**

   The following references provide useful information:

   Confidentiality of Alcohol and Drug Abuse Patient Records, HHS. 42 C.F.R. § 2. Retrieved October 6, 2014 from http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5;node=42%3A1.0.1.1.2.

   Confidentiality of Records. 42 U.S.C. § 290dd-2. Retrieved October 6, 2014 from http://www.gpo.gov/fdsys/pkg/USCODE-2011-title42/pdf/USCODE-2011-title42-chap6A-subchapIII-A-partD-sec290dd-2.pdf.

5. **Consider an area for which there are limited statutory privacy protections (e.g., cell phone data) and discuss how fair information practice principles might or might not apply.**

Exercise B. *Doctors might perform an internet search to find out more information about their patients.*

The following references provide useful information:

Bosch, T. (2013, October 8). Should your doctor be allowed to Google you? *Slate*. Retrieved October 29, 2014 from http://www.slate.com/blogs/future_tense/2013/10/08/should_your_doctor_be_allowed_to_google_you.html.

Warraich, H.J. (2014). When doctors 'Google' their patients. *New York Times*. Retrieved October 29, 2014 from http://well.blogs.nytimes.com/2014/01/06/when-doctors-google-their-patients-2/.

1. **How might looking up information about a patient on the internet alter the doctor-patient relationship?**

2. **Is using the internet to learn more information about patients permissible under the HIPAA Privacy Rule?**

   The following reference provides useful information:

   U.S. Department of Health and Human Services (HHS). (n.d.). Summary of the HIPAA Privacy Rule [Webpage]. Retrieved October 29, 2014 from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/.

   Read the following sections on this page:

   - *What Information is Protected*
   - *General Principle for Uses and Disclosures*
   - *Permitted Uses and Disclosures*
   - *Authorized Uses and Disclosures*
   - *Limiting Uses and Disclosures to the Minimum Necessary*

3. **Does the HIPAA Privacy Rule adequately protect privacy in the doctor-patient relationship? Why or why not?**

4. **When, if ever, might it be appropriate for a patient to be denied medical care because of information obtained from an internet search?**

5. **A person must have a "reasonable" expectation of privacy if they want to claim before a court of law that their privacy rights were violated. Consider how expectations of privacy have changed over time. Can patients reasonably expect their information to remain private if they post personal information on social media sites?**

VII. Glossary of Terms

Anonymized data: Data from which a patient's identifiers have been permanently removed and no link remains between the individual and his or her data.

Autonomy: The capacity to direct the course of one's own life or to live according to one's own values and beliefs.

Confidentiality: A set of rules or a promise to restrict access to certain information.

De-identified data: Data that have been separated from information identifying the individual from which they were derived. Importantly, a "key" or code connecting the two might still exist, but researchers are not allowed to access the key.

Democratic deliberation: An approach to collective and collaborative decision making that seeks to clarify and articulate factual and ethical issues at the core of a debate, to create consensus whenever possible, and to map the terrain of disagreements in a respectful way—when agreement is not immediately attainable—by encouraging reciprocity, respect for persons, transparency, publicity, and accountability.

Distributive justice: An ethical principle that calls for equitable distribution of benefits and burdens across society—for example, the benefits and burdens of biomedical research, or of technological advances.

Informed consent: The process of informing and obtaining permission from an individual before conducting medical or research procedures or tests.

Intellectual freedom and responsibility: The notion that scientists and other researchers, acting responsibly, should use their creative abilities to advance science and the public good while adhering to the ideals of research, avoiding harm to others, and abiding by all associated rules.

Public beneficence: An ethical principle that encourages us to pursue and secure public benefits while minimizing personal and public harm.

Respect for persons: Ethical principle requiring that individuals are treated as independent and self-determining (autonomous) agents and that persons with diminished autonomy are entitled to additional protections.

Responsible stewardship: Ethical principle requiring governments and scientists to proceed prudently in promoting science and technology that can improve human welfare but can also cause harm, and to recognize the importance of citizens and their representatives acting collectively for the betterment of all, especially those who cannot represent themselves.

VIII. Additional Resources

Allen, A.L. (2011). *Privacy Law and Society, 2nd ed*. St. Paul, MN: West/Thomson.

Allen, A.L. (2011). *Unpopular Privacy: What Must We Hide?* New York, NY: Oxford University Press.

Allen, A.L. (1999). Coercing privacy. *William and Mary Law Review*, 40(3), 723-757. Retrieved October 6, 2014 from http://scholarship.law.wm.edu/wmlr/vol40/iss3/3/.

Bosch, T. (2013, October 8). Should your doctor be allowed to Google you? *Slate.* Retrieved October 29, 2014 from

http://www.slate.com/blogs/future_tense/2013/10/08/should_your_doctor_be_allowed_to_google_you.html.

Cate, F.H. (1997). *Privacy in the Information Age*. Washington, DC: Brookings Institution Press.

Confidentiality of Alcohol and Drug Abuse Patient Records, HHS. 42 C.F.R. § 2. Retrieved October 6, 2014 from http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5;node=42%3A1.0.1.1.2.

Confidentiality of Records. 42 USCS § 290dd-2. Retrieved October 6, 2014 from http://www.gpo.gov/fdsys/pkg/USCODE-2011-title42/pdf/USCODE-2011-title42-chap6A-subchapIII-A-partD-sec290dd-2.pdf.

DeCew, J. (2013). Privacy. In E.N. Zalta. (Ed.). *The Stanford Encyclopedia of Privacy*. Retrieved October 6, 2014 from http://plato.stanford.edu/entries/privacy/.

European Commission. (n.d.). Factsheet on the "Right to be Forgotten" ruling (C-131/12). Retrieved October 6, 2014 from http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

Lee, D. (2014, May 13). What is the 'right to be forgotten'? *BBC*. Retrieved October 6, 2014 from http://www.bbc.com/news/technology-27394751.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Pennock, J., and J. Chapman. (Eds.). (1971). *NOMOS XIII: Privacy*. New York, NY: Atherton Press.

Schoeman, F.D. (Ed.). (1984). *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press.

Schwartz, P.M. (2009). Preemption and privacy. *The Yale Law Journal*, 118, 902-947.

U.S. Department of Health and Human Services (HHS). (n.d.). Summary of the HIPAA Privacy Rule [Webpage]. Retrieved October 29, 2014 from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/.

Warren, S.D., and L.D. Brandeis. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193-220.

Warraich, H.J. (2014). When doctors 'Google' their patients. *New York Times*. Retrieved October 29, 2014 from http://well.blogs.nytimes.com/2014/01/06/when-doctors-google-their-patients-2/.